

**THE UNIVERSITY OF TENNESSEE
BOARD OF TRUSTEES**

MINUTES OF THE AUDIT COMMITTEE

**December 18, 2013
Nashville, Tennessee**

The Audit Committee of the Board of Trustees of The University of Tennessee met at 10:00 a.m., CST, December 18, 2013, in the offices of Bradley Arant Boult Cummings in Nashville, Tennessee.

I. CALL TO ORDER

Mr. D. Crawford Gallimore, Chair, called the meeting to order.

II. ROLL CALL

Ms. Sandy S. Jansen, Executive Director, called the roll, and the following Audit Committee members were present:

Mr. D. Crawford Gallimore
Mr. Spruell Driver
Mr. Waymon Hickman, external member
Mr. Tommy Whittaker

Special meeting requirements were reviewed since Trustee Ferguson (ex-officio member) participated by phone.

Ms. Jansen announced the presence of a quorum of the committee. Other members of the administrative staff were present, as well as BerryDunn representatives.

III. APPROVAL OF MINUTES FROM LAST MEETING

Chair Gallimore asked for any corrections to the August 12, 2013, minutes. Hearing none, Mr. Hickman moved approval of the minutes as presented, and Trustee Whittaker seconded the motion. A roll call vote was taken from the committee members on the approval, and it carried unanimously.

IV. INFORMATION TECHNOLOGY SECURITY POSTURE ASSESSMENT

Chair Gallimore provided background on the information technology (IT) security assessment and reminded committee members that the Audit Committee charter enumerates a number of committee responsibilities. One responsibility is to consider the effectiveness of the University's internal control system, including information technology, security, and control. As such, the committee authorized the issuance of a request for proposals to assess the University's security posture and asked Ms. Jansen to lead a team to evaluate the proposals. That team recommended BerryDunn to the committee, and the project was approved in May. BerryDunn has completed its work and prepared a draft report of the results.

Mr. Clint Davies, Mr. David Houle, and Ms. Eigen Heald, representatives from BerryDunn, presented an overview of the IT security posture assessment results (Exhibit 1).

After the presentation, members of the Audit Committee and administration asked the team about the recommendations presented. Chair Gallimore asked about the dual reporting structure and the amount of autonomy each campus should have over its IT processes. He also asked about best practice structures for the reporting relationship between the campuses' chief information officers (CIO) and the UT System CIO.

Mr. Davies explained that opportunities are already in place for the UT campuses to collaborate on information security practices and challenges. This report encourages building on those opportunities. Policies and standards are needed to guide the actions and practices at the campuses. Currently, there is a lack of consistency and standards and no clear authority at the University of Tennessee. He cautioned that the model will not work if it is dictatorial, so the report focuses on collaborative processes. The campuses need to be engaged in the process of developing those standards. Once the standards are set, everyone needs to live by them and be held accountable.

Ms. Heald added that UT has slightly different standards at each campus and the University needs to create structure. Policy statements should be written broadly so the campuses have the opportunity to develop their own plans and procedures. Campuses must comply with the policy and standards and must document and approve exceptions. She added that consequences must be imposed for noncompliance.

Dr. DiPietro asked about the type of consequences the team had seen implemented in instances of noncompliance. Ms. Heald responded that consequences are across the board. She said a monitoring process should be established to review and approve systems before they are purchased to ensure certain standards are met.

Chair Gallimore asked the team about the CIO reporting structure and to whom the CIO reports in other institutions of higher education. Mr. Davies responded that the CIO typically reports to the Office of the President, an operating officer, or senior leader at the system level.

Trustee Ferguson commented that the report's recommendations focused on behavioral, cultural, and procedural issues but did not comment much on software and architecture. He asked whether UT can achieve those acceptable levels of security with the different IT systems at every campus, college, department, and used by individuals connected to the system. He questioned whether the architecture will achieve the level of security needed.

Ms. Heald responded that she believed UT can achieve an acceptable level of security with the current architecture if it is structured. She stated the structure is very loose at the campus level and needs to come from the University System.

Trustee Driver asked about the staffing levels at the Institute for Public Service (IPS). Mr. Houle responded that the CIO at IPS is an army of one. The team discussed the need for additional security staffing during the assessment but felt an opportunity exists to develop service-level agreements, with Knoxville to manage security.

Dr. DiPietro asked whether there was comparative data on the maturity for the peer institutions included in the report. Mr. Houle said the information is not available.

Dr. DiPietro asked if the peer institutions might be more mature because they had more funding and staff. Mr. Houle indicated he did not think that was necessarily the case.

Dr. DiPietro questioned whether the maturity model developed for this assessment was a best practice. Mr. Houle responded that, while the maturity model is using best practices, multiple variations of maturity models are available. Mr. Houle stated most organizations, not just in higher education, have a maturity score ranging from two to three. From that perspective, UT is

not too far from the average. He noted that all institutions of higher education are struggling, not just UT. It is important to look at the maturity model and optimize. Focusing on the right documentation, getting the right language, and accepting a common framework and terminology will move the University along the continuum.

Mr. Peccolo asked the team to speak on the maturity model and how staff imbedded in the applications, such as security people embedded in the IRIS system, were factored into the model. Ms. Heald indicated they considered the embedded security processes. Best practices in software development require a model or framework in which code is created, stored, changed, and promoted. It includes such things as security testing and application-level testing. None of the institutions the team visited had the National Institute of Standards and Technology (NIST) framework clearly defined. Instead, it was ad hoc and intuitive and lacked structure.

Mr. Hickman asked if the present staff members are knowledgeable enough to provide the needed training across the system. Mr. Davies commented that the team found UT to have very knowledgeable staff. Ms. Heald said they received much feedback on the lack of training. Many individuals interviewed felt there was insufficient training. Some individuals stated they received compliance training once a year but nothing else. Based on her work, she indicated a "train the trainer" model might be a challenge because the staff members are very busy. UT can provide numerous types of education that does not have to be presented by University staff (e.g., online training and other resources).

Mr. Houle added that, with UT's multiple entities, coordination and planning must use the same framework for training so that the University gets the best training at the best cost.

Trustee Ferguson asked Dr. DiPietro to share his reactions to the findings and recommendations. Dr. DiPietro indicated he was pleased to hear that UT is in the middle of the pack or the lower part of the middle of the pack, when compared to peers. He commented that it is good to understand the context when considering the scoring of the maturity model. Dr. DiPietro added that he feels the University has been fortunate no major incident has occurred in the last four or five years. He said the University needs to take the recommendations seriously and he plans to meet with the chancellors to move forward. Then we need to get a strategy to allow UT to have more confidence about the security of the operation. The cost benefit has to be evaluated and the policy side is not that costly, so he felt getting the policies in place and having the Board engaged at a

high level through the Audit Committee was a good place to start. Once the policies are in place and things are reviewed routinely, the University must examine the cost benefit of the more costly items to be implemented. The associated risk should be considered when deciding whether to make an investment in one area as opposed to another. Dr. DiPietro said the report is well done, lengthy, and substantive. He added that the University probably cannot afford to do all of it and will have to eat this elephant a bite at a time over the next few years.

Chair Gallimore asked the team to comment on priorities for the University. Mr. Davies commented that working on the organization and the policy issues would be a first priority. Staff are in place on the campuses who are thinking about security and trying their best; however, they need to be given some structure. Mr. Davies said some existing environmental security issues could be addressed. Chair Gallimore indicated that the committee would want them addressed immediately because those fixes are relatively easy.

Dr. DiPietro and Mr. Houle discussed the staffing at the Institute of Agriculture (UTIA). Mr. Houle indicated UTIA is doing good work right now. They are moving forward quickly on their maturity and strengthening classification, and the CIO is doing a good job to move this forward. Based on where the team saw UTIA and its long-term needs, the team felt the institute should have a permanent position.

Dr. DiPietro asked about the county interface with UTIA. Ms. Heald noted there is a crossover with IT and some components of IT security.

Trustee Driver asked if the team had any insight on using cyber liability risk insurance regarding third-party suppliers who may have access to the University's information systems. Ms. Heald responded that the best insurance is good oversight and that the insurance requires certain baselines and security controls to be in place. Mr. Houle added that insurance would not totally mitigate the reputational risks associated with security.

Chair Gallimore stated the Audit Committee looked forward to updates on the progress.

Trustee Whittaker commented that overall he felt the report sounded good because it seemed many of the areas could be addressed without spending lots of money. He realized that numerous things needed to be done, but the report was encouraging.

Trustee Ferguson asked if there would be follow-up on the actions management plans to take to address the recommendations. Dr. DiPietro and Ms. Jansen agreed that Audit and Consulting Services (ACS) would follow up and updates would be presented at future Audit Committee meetings.

V. UT KNOXVILLE COMPLIANCE RISK MANAGEMENT EFFORT

Dr. Taylor Eighmy, Vice Chancellor for Research and Engagement, provided an update (Exhibit 2). He reported on the ongoing status, along with the approach for moving forward.

At the end of the presentation, Chair Gallimore asked Dr. Eighmy to share areas of risk that concern him. Dr. Eighmy commented that lab safety requires attention because of unfortunate accidents that can occur in laboratories. He indicated he believes UT has a good system in place; however, because of previous experience, he is sensitive to problems in that area.

Mr. Hickman asked about liability with the UT hospital. There was discussion that, while it is a separate entity, reputational risk does exist.

VI. EMERGENCY MANAGEMENT

Mr. Mark Smith, Director of Environmental Health and Safety, provided a report on emergency management (Exhibit 3).

Following the presentation, Dr. DiPietro asked what activities were happening in Chattanooga to mitigate bomb threats. Mr. Smith responded that the topic had been discussed at the last emergency management meeting. There were discussions about alternate locations so that if a bomb threat came for one building, students could move to an alternate location. He added that Chattanooga has a plan to reduce disruption.

Trustee Driver asked about using instant messaging and texting to students. There was discussion about the campus's use of texting for emergencies. It was confirmed that students would receive a text message in an event such as an active shooter. Mr. Smith clarified that it was good to have redundancy built in so that the University does not rely on one method of communication.

VII. APPROVAL OF INTERNAL AUDIT AND AUDIT COMMITTEE CHARTERS

Ms. Jansen presented the Internal Audit and Audit Committee Charters as required by audit standards and by the charters. Ms. Jansen reviewed the section on the administrative reporting relationship. She commented that independence is fostered and adequate resources in terms of staff and budget are provided. She stated Mr. Peccolo does not interfere with the audit work, does not try to improperly influence ACS, and does not interfere with independence and objectivity. No changes were recommended.

Mr. Hickman moved approval of the charters (Exhibit 4). Trustee Whittaker seconded the motion. A roll call vote was taken from the committee members on the approval, and it carried unanimously.

VIII. UNIVERSITY'S FINANCIAL RISK ASSESSMENT

Ms. Sandy Jansen presented the University's financial risk assessment (Exhibit 5).

Ms. Jansen commented that, consistent with last year's risk assessment, the human resources processes are at the top of the risk assessment. Some new risks were identified in the human resources process. Because of the risks, an audit is planned in 2014 to review human resources onboarding. This audit may address some of the risks identified during the risk assessment in the last couple years, including failure to adequately train and develop employees, delays in the hiring process, failure to file paperwork timely, and failure to mitigate identity theft. The other area of note on the risk assessment was the procurement process. A project is being carried over to 2014 to examine the invoicing process.

IX. 2013 ANNUAL AUDIT PLAN STATUS

Ms. Jansen presented the 2013 audit plan (Exhibit 6) and provided an update of the work being conducted.

The ACS team made progress on the engagements in progress from prior years. Twenty-nine of the engagements in progress on January 1, 2013, were completed. The remaining two (one planned and one investigation) will be completed in early 2014.

For required and risk-based engagements, two new engagements were added and seven were cancelled during the year because of changing risks and other priorities. Fifteen of the required or risk-based engagements were issued or will

be issued by year-end. The remaining engagements are in progress or will be carried forward to calendar year 2014. The team refined the process to conduct departmental audits and will continue this work in 2014.

In addition to the prior-year and planned audit engagements, fourteen investigations were completed and four are in progress.

Chair Gallimore asked Ms. Jansen to speak about current staffing. Ms. Jansen explained that all positions were filled except for an audit manager position in Chattanooga. The position will be a key hire because the office has been understaffed. She commented that, with the growth on that campus, risks have increased and the office needs to provide more coverage. The office has been trying to provide coverage with supervision from Knoxville, but a manager is needed on the Chattanooga campus.

X. APPROVAL OF 2014 AUDIT PLAN AND COMPLIANCE PLAN

Ms. Jansen presented the 2014 Audit Plan and Compliance Plan for approval.

Trustee Whittaker moved approval of the plan (Exhibit 7). Mr. Hickman seconded the motion. A roll call vote was taken from the committee members on the approval, and it carried unanimously.

XI. DISCRETIONARY EXPENDITURE REPORT

Ms. Jansen presented the discretionary expenditure report (Exhibit 8).

XII. TRAVEL EXCEPTION REPORT

Ms. Jansen presented the travel exception report (Exhibit 9), and no exceptions were noted.

XIII. HOUSING EXCEPTION REPORT

Ms. Jansen presented the housing exception report (Exhibit 10), and no exceptions were noted.

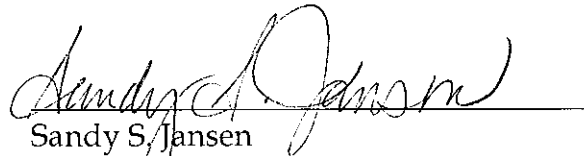
XIV. OTHER BUSINESS

The Chair called for any other business to come before the Audit Committee. There was none.

XV. ADJOURNMENT

There being no further business to come before the Audit Committee in public session, the meeting was adjourned.

Respectfully Submitted,

A handwritten signature in cursive script, reading "Sandy S. Jansen", written over a horizontal line.

Sandy S. Jansen
Executive Director
Audit and Consulting Services